EXAMINER'S AMENDMENT

1. The application has been amended as follows:

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with applicant's attorney on 06-15-2009.

Claims are amended as follows:

As per claim 17,

A method for verifying validity of a network key in a digital domestic network, communicating with ~~comprising~~ at least a broadcasting device and at least one processing device, the broadcasting device ~~transmits to the processing device encrypted data~~ having encrypted data to broadcast to the processing device, ~~the data being accessible by the processing device due to a network key unknown by the broadcasting device,~~ the method comprising:

providing the encrypted data accessible by the processing device due to a network key unknown by the broadcasting device;

transmitting by the broadcasting device a test key to the processing device, receiving from the processing device a cryptogram made up of the test key encrypted by the network key, and

determining the validity of the network key by comparing the received cryptogram with at least one of a plurality of control cryptograms taken from a list of control data generated by a verification center for the test key,

wherein the control cryptograms are in a black list containing cryptograms obtained by encrypting the test key with invalid network keys and in a white list containing the cryptograms obtained by encrypting the test key with valid network keys.

As per claim 24,

The method according to claim [[22]] 17, wherein an error signalization inviting the user to change the terminal module is generated when a received cryptogram is present in the black list and refused during the comparison.

As per claim 33,

The method according to claim [[23]] 17, wherein an error signalization inviting the user to change the terminal module is generated when a received cryptogram is absent of the white list and refused during the comparison.

Claims 22, 23 and 34 are cancelled.

Allowable Subject Matter

2. Claims 17, 18, 20, 21, 24-33, 35 and 36 are allowed.

The following is an examiner's statement of reasons for allowance:

Claims are allowed in the light of applicant's arguments in the Remarks of 03-26-2009, (on page 12-13 as shown below):

> "[i]n contrast, the claimed invention may be carried out in a case that the server has no access to the secret key, e.g., a third party having authority may issue a list of cryptograms as well as their corresponding test keys for verification. [t]he list may be transferred to the broadcasting device for further verification. **[h]ence, it is noted that at no time, the network keys are stored in the broadcast device**. [a]ccordingly, in order to verify a network key, without having the network key itself, the broadcasting device sends a test key to the processing device. [t]he processing device responds with a cryptogram, i.e., a test key encrypted by its network key. **[t]he broadcasting device can then compare the received cryptogram with the expected cryptogram received previously by the authority**. [t]herefore, the indirect verifying validity of the network key by the cryptograms provided by an authority is not disclosed in the Togirai reference".

Calms are allowable in the light of the following claim limitations:

> "determining the validity of the network key by comparing the received cryptogram with at least one of a plurality of control cryptograms

taken from a list of control data generated by a verification center for the test key, wherein the control cryptograms are in a black list containing cryptograms obtained by encrypting the test key with invalid network keys and in a white list containing the cryptograms obtained by encrypting the test key with valid network keys".

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali Abyaneh whose telephone number is (571) 272-7961. The examiner can normally be reached on Monday-Friday from (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on **(571) 272-3865**. The fax phone numbers for the organization where this application or proceeding is assigned as (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/A. S. A./

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437